(12) UK Patent Application (19) GB (11) 2 371 898 (13) A

(43) Date of A Publication 07.08.2002

(21) Application No 0125203.0

(22) Date of Filing 19.10.2001

(30) Priority Data
(31) 01005038 (32) 02.02.2001 (33) KR

(51) INT CL[7]
G06F 17/60 , H04L 29/06

(52) UK CL (Edition T)
G4A AAP

(56) Documents Cited
WO 2000/062232 A1 WO 2000/027067 A1

(58) Field of Search
UK CL (Edition T) G4A AAP
INT CL[7] G06F , H04L
ONLINE:WPI,EPODOC,JAPIO,TDB,INSPEC,XPESP

(71) Applicant(s)
Stom C&C Inc
(Incorporated in USA - New York)
110 East 55th Street 16th, New York, NY 10022,
United States of America

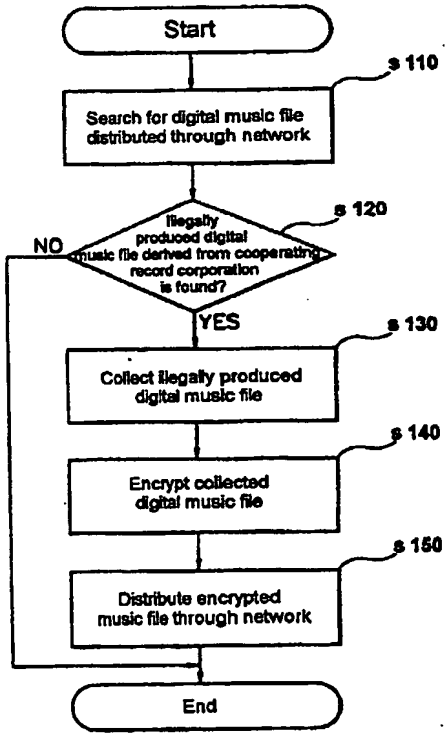
(72) Inventor(s)
Cheol-Woong Lee
Chang-Young Lee

(74) Agent and/or Address for Service
Stevens Hewlett & Perkins
Halton House, 20/23 Holborn, LONDON, EC1N 2JD,
United Kingdom

(54) Abstract Title
Preventing unauthorised distribution of digital material (eg music) through a communication network by encryption or watermarking of any material found

(57) A method of preventing reduction of record sales due to a digital music file being illegally distributed through a communication network is disclosed. The method comprises a) collecting an illegally produced digital music file, which is derived from a record of a cooperating record corporation by searching the network (s110), b) encrypting the collected digital music file with a predetermined key (s140); and c) redistributing the encrypted digital music file through the network (s150). According to present invention, the method collects the illegally produced (or reproduced) digital music file that is shared and distributed through the network, encrypts the collected music file, and enables only users having a private key to use the digital music files, thus inducing the users habitually using the digital music files to use them after paying a justifiable fee and being assigned the encryption key, and to purchase the formal record. Watermarking may be used instead of encryption.

Fig. 2



GB 2 371 898 A

BEST AVAILABLE COPY

Fig. 1

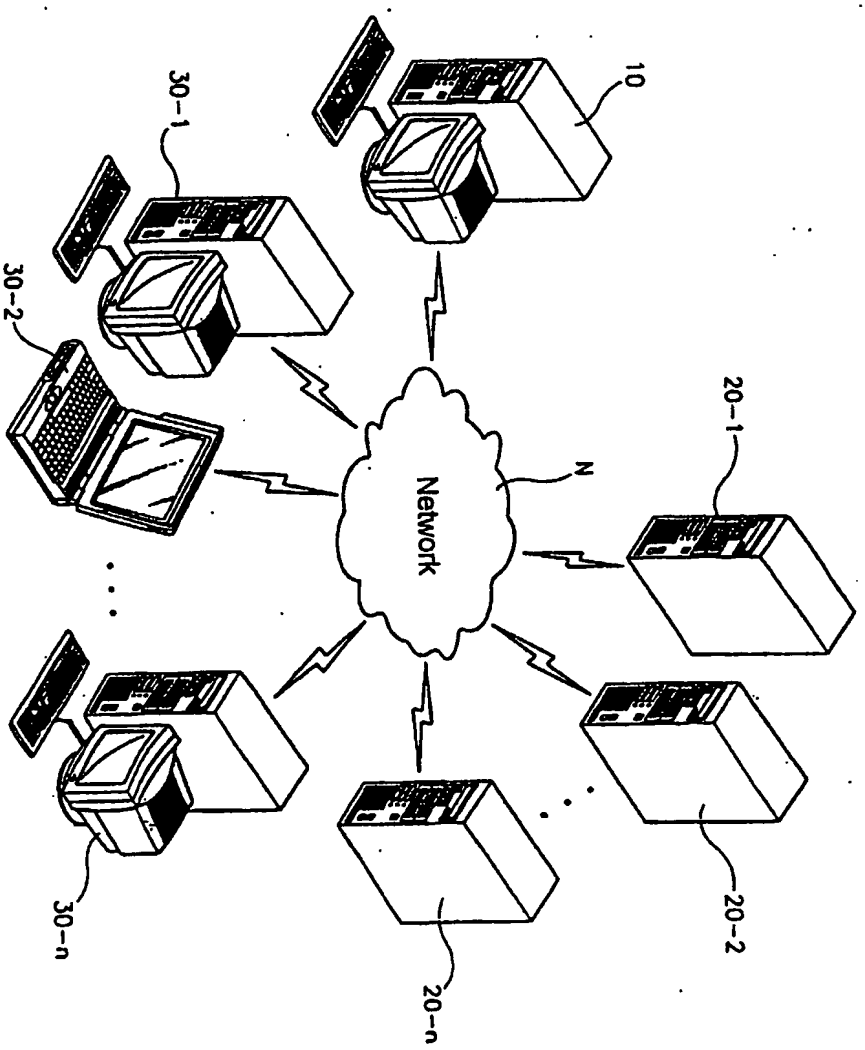


Fig. 2

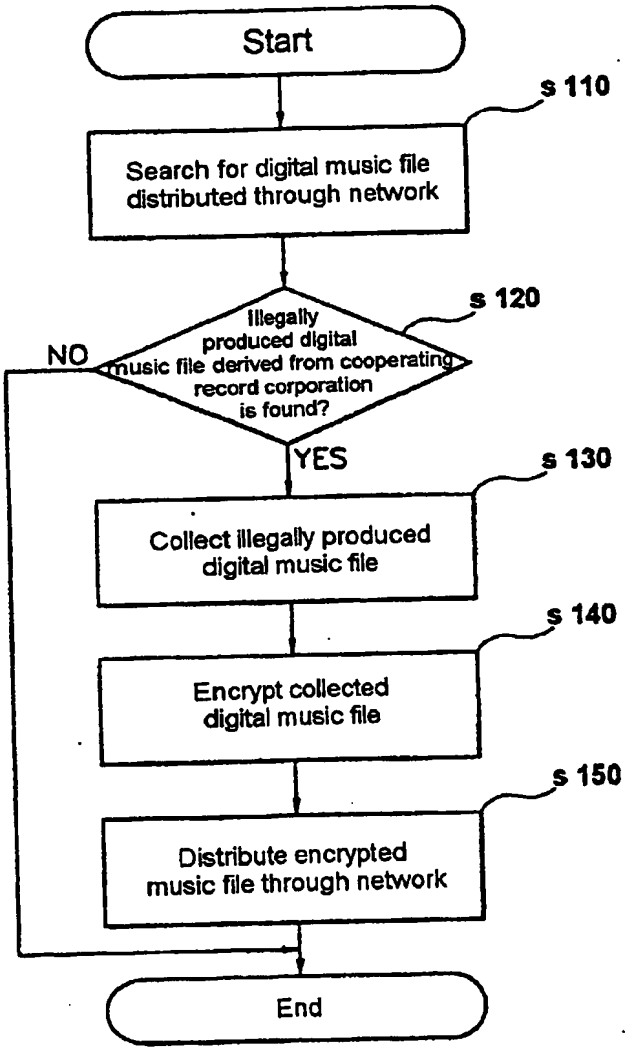

Start
s 110
Search for digital music file distributed through network
s 120
Illegally produced digital music file derived from cooperating record corporation is found?
NO
YES
s 130
Collect illegally produced digital music file
s 140
Encrypt collected digital music file
s 150
Distribute encrypted music file through network
End

Fig. 3

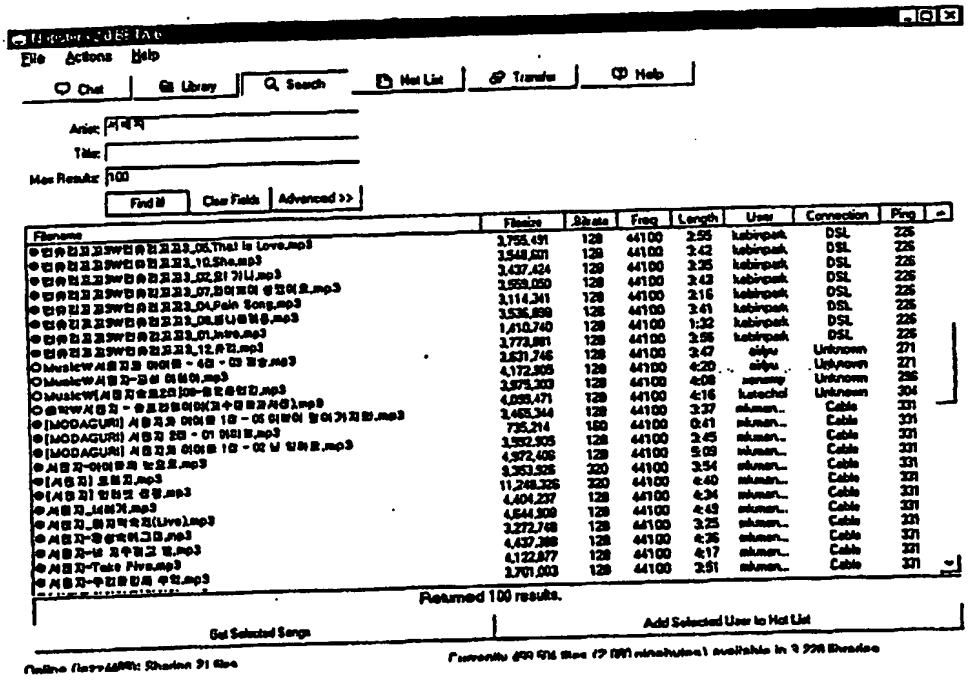

File Actions Help
Chat
Library
Search
Hot List
Transfer
Help
Artist:
Title:
Max Results: 100
Find It!
Clear Fields
Advanced >>
Filename
Filesize
Bitrate
Freq
Length
User
Connection
Ping
Returned 100 results.
Get Selected Songs
Add Selected User to Hot List

Fig. 4

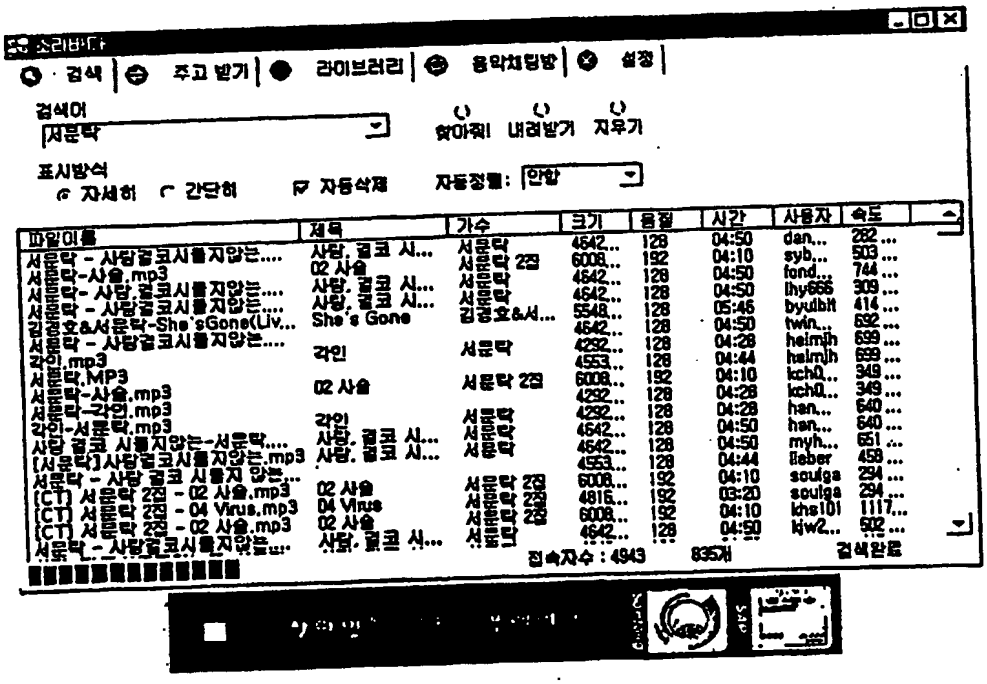

검색
주고 받기
라이브러리
음악채팅방
설정
검색어
서문탁
찾아줘!
내려받기
지우기
표시방식
자세히
간단히
자동삭제
자동정렬:
한함
파일이름
제목
가수
크기
음질
시간
사용자
속도
서문탁 - 사랑결코시들지않는....
서문탁-사슬.mp3
서문탁- 사랑,결코시들지않는....
서문탁 - 사랑결코시들지않는....
김경호&서문탁-She'sGone(Liv...
서문탁 - 사랑결코시들지않는....
각인.mp3
서문탁.MP3
서문탁-사슬.mp3
서문탁-각인.mp3
각인-서문탁.mp3
사랑 결코 시들지않는-서문탁....
[서문탁]사랑결코시들지않는.mp3
서문탁 - 사랑 결코 시들지 않는...
(CT) 서문탁 2집 - 02 사슬.mp3
(CT) 서문탁 2집 - 04 Virus.mp3
(CT) 서문탁 2집 - 02 사슬.mp3
서문탁 - 사랑결코시들지않는....
사랑, 결코 시...
02 사슬
사랑, 결코 시...
사랑, 결코 시...
She's Gone
각인
02 사슬
각인
사랑, 결코 시...
사랑, 결코 시...
02 사슬
04 Virus
02 사슬
사랑, 결코 시...
서문탁
서문탁 2집
서문탁
서문탁
김경호&서...
서문탁
서문탁 2집
서문탁
서문탁
서문탁
서문탁 2집
서문탁 2집
서문탁 2집
서문탁
접속자수 : 4943
835개
검색완료

Fig. 5

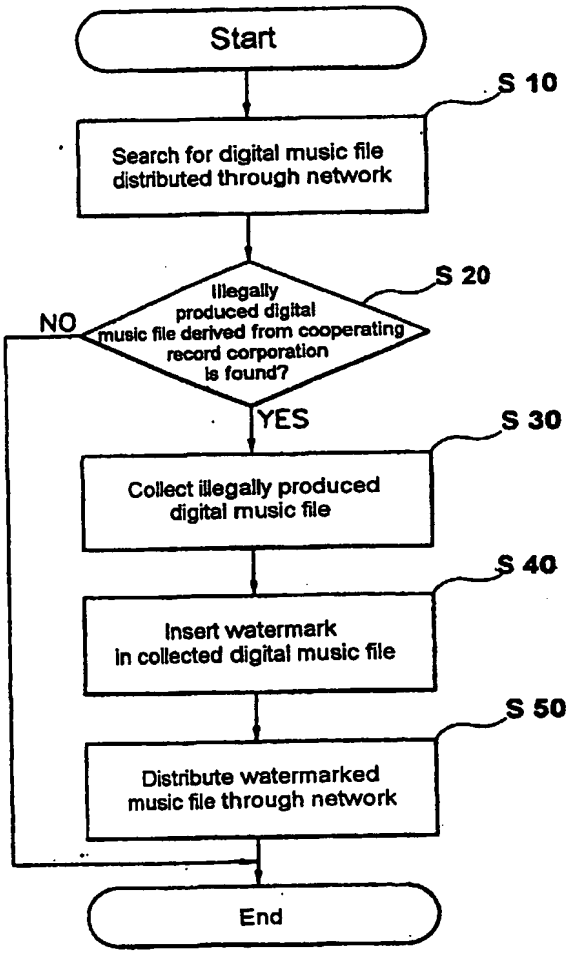

Start
S 10
Search for digital music file distributed through network
S 20
Illegally produced digital music file derived from cooperating record corporation is found?
NO
YES
S 30
Collect illegally produced digital music file
S 40
Insert watermark in collected digital music file
S 50
Distribute watermarked music file through network
End

Fig. 6a

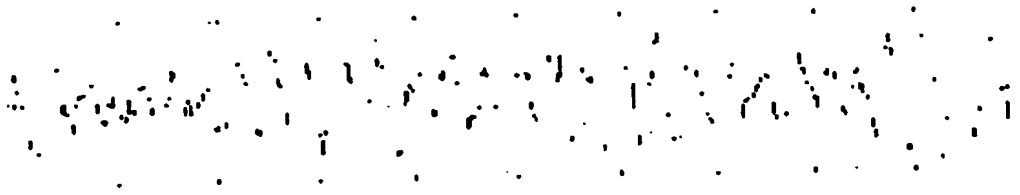
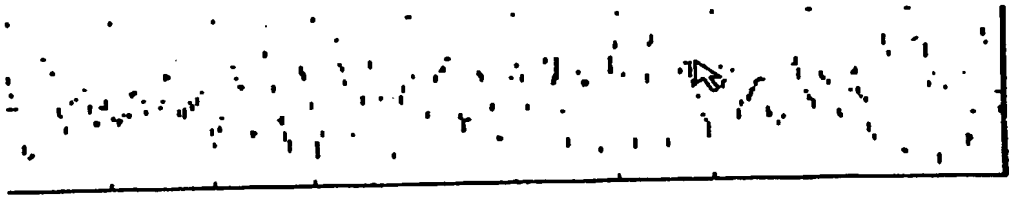


Fig. 6b



METHOD OF PREVENTING REDUCTION OF RECORD SALES DUE TO DIGITAL MUSIC FILES BEING ILLEGALLY DISTRIBUTED THROUGH A COMMUNICATION NETWORK

The present invention relates in general to a method of preventing reduction of sales amount of records due to a digital music file illegally distributed through a communication network, and more particularly to a method which allows sharing and distributing of a digital music file employing a security technique, such that it can restrain a user from holding and using a digital music file illegally reproduced and thus prevent the reduction of sales amount of records due to the digital music file illegally distributed through a communication network.

Generally, a record corporation sells a record produced by recording an analog or digital signal on a medium such as a cassette tape or an optical disc(e.g. long play disc or compact disc).

As digital audio-concerned techniques have been developed, many softwares and hardware devices have been

developed for forming an analog or digital signal recorded onto a medium as a digital-format music file such that it can be stored or copied easily with a digital device(e.g. personal computer terminal), and freely reproduced from the device.

The digital-format music file generated by the softwares or hardware devices is easily propagated through a communication network due to its characteristic of simplicity in reproducing and transmitting. Especially, a digital music file with MP3(MPEG1 layer 3) format, which recently has gained great popularity, has a data size smaller than that of a conventional digital music file by 90 to 92%, while its sound quality is as high as an original sound recorded in the medium(for example, compact disc) by using an audio compression technique of MPEG 1. For this reason, a large quantity of digital music files with MP3 format have been illegally reproduced through the communication network.

Moreover, many programs or services such as "Napster" or "Soribada" for sharing digital music files with data format such as MP3 between different users using a P2P(peer to peer) method have been proposed and popularized among users recently. Thus, a search and reproduction of the digital music file through the communication network are gradually becoming easier and more simplified, and thus the users of the programs or the services are progressively increased in number.

Consequently, the conventional digital music file is disadvantageous in that reproduction of the digital music file infringes illegally a copyright of the music and causes sales amount of records to be reduced.

Therefore, the present invention has been made in view of the above problem, and it is an object of the present invention to provide a method of preventing reduction of sales amount of records due to digital music files illegally distributed through communication network, which collects digital music files shared or distributed through the shared server or program, applies a security technique for restraining users from using the digital music files without permission, and shares or redistributes the digital music file with security through the network, thus preventing users from sharing and using the music files reproduced illegally.

In accordance with one aspect of the present invention, there is provided a method of preventing unauthorised distribution of a digital music file through a communication network, comprising: a) collecting an illegally produced digital music file, which is derived from a record of a cooperating record corporation, by searching the network, b) encrypting the collected digital music file with a predetermined key; and c) redistributing the encrypted digital music file through the network.

In accordance with another aspect of the present invention, there is provided a method of preventing reduction of record sales due to a digital music file being illegally distributed through a communication network, comprising: a) collecting an illegally produced digital music file, which is derived from a record of a cooperating record corporation, by searching the network, b) inserting a watermark containing a predetermined secret information in the collected digital music file, and c) redistributing the watermarked digital music file through the network.

The above and other objects, features and advantages of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 is block diagram showing a system for performing a method of preventing reduction of sales amount of records due to a digital music file being illegally distributed through a communication network;

Fig. 2 is a flowchart showing a method of preventing reduction of sales amount of records due to a digital music file being illegally distributed through a network;

Fig. 3 and Fig. 4 are views of examples showing a search for an illegally produced digital music file using a well-

known music file sharing program;

Fig. 5 is a flowchart showing a method according to another preferred embodiment of this invention; and

Fig. 6a and 6b are waveform examples showing an insertion of watermark in the original digital music file.

Fig. 1 is a block diagram showing a system for performing a method of preventing reduction of sales amount of records due to a digital music file illegally distributed through the communication network. Referring to Fig. 1, the system comprises a searching and editing terminal 10, music file sharing servers 20-1~20-n, music file user terminals 30-1~30-n, and a network N. The terminals 10, 30-1~30-n and the servers 20-1~20-n are commonly connected to the network N such as an Internet through various well-known devices like a modem or router, and various methods. The construction and operation of the terminals 10, 30-1~30-n and the servers 20-1~20-n is well known in the field and further explanation is thus not deemed necessary.

The searching and editing terminal 10 searches for the illegally produced digital music file, which is shared or distributed through the network, collects the searched music file, applies a security technique to the collected music

files, and shares and distributes the secured digital music file through the network N.

The searching and editing terminal 10 includes a general hardware device(not shown) included in a computer system, such as a main processor, a network adapter, a display adapter, a main memory and an auxiliary memory, and an operating system(OS), and a program tool for applying the security technique such as a public key encryption algorithm and watermarking algorithm to the digital music file. The specific construction and operation of the terminal 10 is well known in the field and further explanation is thus not deemed necessary.

Further, a plurality of music file sharing programs generally used on the network N are installed at the searching and editing terminal 10 in order to search for the digital music files shared and distributed through the network N.

The music file sharing servers 20-1~20-n search another user's terminal connected to the network N for a corresponding digital music file according to requests from the music file user terminals 30-1~30-n, and connect the user terminals 30-1~30-n so as to enable the users to share the digital music files with each other.

The music file user servers 30-1~30-n operate to share the digital music files through the network N and exchange them through the user terminals 30-1~30-n. The music file

user servers 30-1~30-n include general hardware devices(not shown) installed in a computer system, such as a main processor, a network adapter, a display adapter, a main memory and an auxiliary memory, and an operating system(OS), and at least one of music file sharing programs for sharing the music files between users through the network N.

Hereinafter, an operation sample of the present invention having the construction above will be described in detail referring to the accompanying drawings.

Fig. 2 is a flowchart showing a method of preventing reduction of sales amount of records due to a digital music file illegally distributed through a communication network of this invention.

Referring to Fig. 2, a plurality of the digital music files distributed on the network N are searched for by the searching and editing terminal 10 connected to the network N at step S110. At this time, the searched digital music file is the music file derived from a record of the cooperating record corporation, and the digital music file can be searched by a generally used file sharing program. Preferably, the sharing program has a relatively high recognition degree among the users and wide popularization, and is used to search for the music file.

For example, Fig. 3 and Fig. 4 are views displaying searching for the music file shared on the network N by the

widely popularized music file programs such as "Napster" or "Soribada".

If the illegally produced music file derived from the record of the cooperating record corporation is found at step S120 according to the searching result at step S110, the found digital music file is collected according to the kinds of music at step S130. Generally, one digital music file per a piece of music is collected. However, if necessary, a plurality of music files per a piece of music can be collected.

According to the kinds of music, if only some part of the music files shared on the network N are collected, it is preferable to collect one among the shared music files in which many copies of the same file have the same name, size and playing time. The greater the numbers of the music file with a same name, size and playing time, the higher probability of its being reproduced later by another user, due to its wide distribution through the network to many users.

Next, the collected digital music file is encrypted according to a well-known encryption algorithm at step S140. Here, it is possible to use any one of a well-known symmetric key encryption algorithms and the public key encryption algorithms, however it is preferable to adopt a public key encryption algorithm, considering a division of the keys.

Generally, a public key encryption algorithm called

"Asymmetric key encryption algorithm" is characterized in that it uses different two keys for encryption and decryption. One of the keys is called a private key and the other is called a public key. Typically, the public key is used in encryption and the private key is used in decryption.

Providing that the public key encryption algorithm is adopted to the present invention, the collected digital music file is encrypted with a pubic key authenticated at an authentication organ, such that only the user having a private key can decrypt the digital music file.

The encrypted digital music file is redistributed through the network N at step S150. In this case, the edited digital music file can be distributed using a widely popularized music file sharing program such as "Napster" or "Soribada", thus enabling sharing of the music file with the normal users equally over the network N.

If the digital music file is shared on the network N, the users not having the private key cannot decrypt the digital music file, thereby inducing the user wishing to be assigned the private key to pay a justifiable fee to a corresponding record corporation, or to purchase the formal record.

Hereinafter, another preferred embodiment according to the present invention is described in detail referring to Fig. 5. Fig. 5 is a flowchart showing another preferred embodiment of this invention.

First, a plurality of the digital music files distributed on the network N are searched for by the searching and editing terminal 10 connected to the network N at step S10. At this time, the searched digital music file is the music file derived from a record of the cooperating record corporation, and the digital music file can be searched by a generally used file sharing program. Preferably, the file sharing program has a relatively high recognition degree among the users and wide popularization, and is used to search for the music file.

As described above, Fig. 3 and Fig. 4 are views displaying searching for the music file shared on the network N by the widely popularized music file programs such as "Napster" or "Soribada".

If the illegally produced music file derived from the record of the cooperating record corporation is found at step S20 according to the searching result at step S10, the found digital music file is collected according to the kinds of music at step S30. Generally, one digital music file per a piece of music is collected. However, if necessary, a plurality of music files per a piece of music can be collected.

According to the kinds of music, if only some part of the music files shared on the network N are collected, it is preferable to collect one among the shared music files in which many copies of the same file have the same name, size

and playing time. The greater the numbers of the music file with a same name, size and playing time, the higher probability of its being reproduced later by another user, due to its wide distribution through the network to many users.

Next, a watermark is inserted in the collected digital music file according to a well-known watermarking algorithm at step S40. In this case, the watermark can include some possession information of a writer or a record corporation, or information of a company executing the watermarking and watermark inserting date information, and etc.

As a reference, Fig. 6a shows a waveform of a predetermined original digital file, and Fig. 6b shows the digital file inserted with the watermark in the original digital file(refer to a position of arrow).

Then, the watermarked digital music file is distributed through the network N at step S50. In order to distribute the watermarked digital music file over the network N, a popular music file sharing program(e.g. "Napster" or "Soribada") is used, thus sharing the music file with the normal users equally.

If the watermarked digital music file is shared on the network N, it is possible to call the users unlawfully using the illegally produced(reproduced) digital music file and a service provider enabling its sharing(e.g. a service provider distributing a service program such as "Napster" or "Soribada"

and managing a sharing server) to legal account for illegal reproduction or usage of the music file. If these facts are known to the users, there is an effect of restraining the users from sharing and using the illegal digital music file. Further, through this effect the user listening to the illegally reproduced digital music file is induced to purchase the formal record.

As described above, only the case of sharing and searching the digital music file, which is generated and edited for publicity through the agent server such as "Napster" or "Soribada" is described, but the present invention is not restricted. Further, a program for sharing and searching the digital music file by directly connecting between the users using the P2P without the agent server such as "Gnutella" can be applied to the present invention. It also should be noted that the present invention could be easily applied to a case of downloading a digital music file through a web site.

As apparent from the above description, the present invention provides a method of collecting the illegally produced(or reproduced) digital music file that is shared and distributed through the network, encrypting the collected music file, and enabling only users having a private key to use the digital music files, thus inducing the users habitually using the digital music files to use them after

paying a justifiable fee and being assigned the encryption key, and to purchase the formal record.

Further, the present invention inserts the watermark in the illegally produced digital music file collected through the network, thus restraining the users from sharing and using the illegal digital music files.

Although the preferred embodiments of the present invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that various modifications, additions and substitutions are possible, without departing from the scope of the invention as disclosed in the accompanying claims.

CLAIMS

1. A method of preventing unauthorised distribution of a digital music file through a communication network, comprising:

a) collecting an illegally produced digital music file, which is derived from a record of a cooperating record corporation, by searching the network;

b) encrypting the collected digital music file with a predetermined key; and

c) redistributing the encrypted digital music file through the network.

2. The method as set forth in claim 1, wherein at step a) and c) the collection and distribution of the digital music file are performed by using a popular digital file sharing program.

3. The method as set forth in claim 1, wherein at step a) and c) the collection and distribution of the digital music file are performed by using a popular digital file sharing server.

4. The method as set forth in any one of claim 1 to claim 3, wherein at step b) the collected digital music file

is encrypted by a public key encryption algorithm.

5. A method of preventing reduction of record sales due to a digital music file being illegally distributed through a communication network, comprising:

a) collecting an illegally produced digital music file, which is derived from a record of a cooperating record corporation, by searching the network;

b) inserting a watermark containing a predetermined secret information in the collected digital music file; and

c) redistributing the watermarked digital music file through the network.

6. The method as set forth in claim 5, wherein at step a) and c) the collection and distribution of the digital music file are performed by using a popular digital file sharing program.

7. The method as set forth in claim 5, wherein at step a) and c) the collection and distribution of the digital music file are performed by using a popular digital file sharing server.

8. A method substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office
PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
INVESTOR IN PEOPLE

Application No: GB 0125203.0
Claims searched: 1-8

Examiner: D Midgley
Date of search: 7 May 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): G4A AAP

Int Cl (Ed.7): G06F,H04L

Other: ONLINE:WPI,EPODOC,JAPIO,TDB,INSPEC,XPESP

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A	WO 0062232 A1 (DIGITAL MEDIA)	1,5
A	WO 0027067 A1 (BOCCON-GIBOD)	"

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record.

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.